SYSTEM AND METHOD FOR ANALYZING PROTOCOL STREAMS FOR A SECURITY-RELATED EVENT

ABSTRACT OF THE DISCLOSURE

A system and method are disclosed for analyzing a network protocol stream for a security-related event. At least two states associated with the network protocol in which a first host system communicating with a second host system using the network protocol may be placed are identified. At least one valid transition between a first state of the at least two states and a second state of the at least two states is defined. The at least one valid transition is expressed in the form of a regular expression. The regular expression is used to analyze the network protocol stream.